



**UNITED STATES DEPARTMENT OF COMMERCE**  
**Patent and Trademark Office**

Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. |
|-----------------|-------------|----------------------|---------------------|
| 08/527,382      | 09/12/97    | COSS M               | 1 1 1               |

LM21/1227

JOSEPH B RYAN  
RYAN AND MASON, L.L.P.  
90 FOREST AVENUE  
LOCUST VALLEY NY 11560

EXAMINER  
CROCKETT, R

|                  |              |
|------------------|--------------|
| ART UNIT<br>2787 | PAPER NUMBER |
|------------------|--------------|

DATE MAILED: 12/27/99

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

# Office Action Summary

Application No.  
**08/927,382**

Applicant(s)  
**Coss et al.**

Examiner  
**Robert Crockett**

Group Art Unit  
**2787**



☒ Responsive to communication(s) filed on Nov 12, 1999

☒ This action is **FINAL**.

☐ Since this application is in condition for allowance except for formal matters, **prosecution as to the merits is closed** in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire 3 month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

## Disposition of Claims

☒ Claim(s) 1-26 is/are pending in the application.

Of the above, claim(s) \_\_\_\_\_ is/are withdrawn from consideration.

☐ Claim(s) \_\_\_\_\_ is/are allowed.

☒ Claim(s) 1-26 is/are rejected.

☐ Claim(s) \_\_\_\_\_ is/are objected to.

☐ Claims \_\_\_\_\_ are subject to restriction or election requirement.

## Application Papers

☐ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☐ The drawing(s) filed on \_\_\_\_\_ is/are objected to by the Examiner.

☐ The proposed drawing correction, filed on \_\_\_\_\_ is ☐ approved ☐ disapproved.

☐ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

## Priority under 35 U.S.C. § 119

☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

☐ All ☐ Some\* ☐ None of the CERTIFIED copies of the priority documents have been  
☐ received.

☐ received in Application No. (Series Code/Serial Number) \_\_\_\_\_.

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\*Certified copies not received: \_\_\_\_\_

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

## Attachment(s)

☐ Notice of References Cited, PTO-892

☒ Information Disclosure Statement(s), PTO-1449, Paper No(s). 7

☐ Interview Summary, PTO-413

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

--- SEE OFFICE ACTION ON THE FOLLOWING PAGES ---

### PART III. DETAILED ACTION

#### *Drawings*

1. This application has been filed with informal drawings which are acceptable for examination purposes only. Formal drawings will be required when the application is allowed.

#### *Claim Rejections - 35 USC § 103*

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-26 are rejected under 35 USC 103(a) as being unpatentable over Shwed (US 5606668).

As per claims 1-7, 17-21, and 22-26, Shwed (US 5606668) describes a security system for a computer network that implements packet filtering (column 3, lines 59-65). Shwed teaches that his system applies a particular security rule to an incoming packet (column 7, lines 14-24) based on data extracted from the incoming packet (column 8 lines 39-49 and Fig 8).

As per claim 1, Shwed does not explicitly teach that his system derives a session key for the incoming packet. However, processing the extracted packet data in the Shwed invention (column 8, line 39 to column 9, line 63) would have been recognized by one of ordinary skill in the art, at the time the invention was made, as an obvious equivalent to deriving a session key for the incoming packet, because a session key indicates which security rule to use for a particular packet. Shwed further teaches that a specific TCP destination port may be among the data extracted from the incoming packet (columns 9, line 64 to column 10, line 14). Shwed further teaches that his system is implemented using gateways having multiple network interfaces (Fig 2), where the gateway is connected through a router to the Internet.

As per claims 2, 3, 4, 5, 19, 21, 24, and 26, Shwed does not explicitly teach that his invention processes all types of Internet protocol packets, such as UDP packets, or all useful packet data, such as IP addresses. However, the Internet was well-known to those of ordinary skill in the art, at the time the invention was made, to utilize layered communication protocols, including UDP in addition to TCP, and it was also well-known to those skilled in the art that methods used to extract data from the headers of TCP packets could be utilized to extract data from UDP packets as well, and that these methods could have been utilized to extract many types of packet header information, including source address, destination address, next-level protocol, source port, and destination port data.

It would have been obvious to one skilled in the art, at the time the invention was made, to program the Shwed invention to process all types of Internet protocol packets and to extract all useful packet header data to assist in security rule decision making, because

this would have been easy to accomplish within the Shwed system and would enable the Shwed system to meet a wide range of user security requirements.

As per claims 6, 7, 18, 20, 23, and 25, Shwed teaches that his system is implemented using gateways having multiple network interfaces (Fig 2), where the gateway is connected through a router to the Internet. Gateways were well-known to those of ordinary skill in the art, at the time the invention was made, to allow packets to be routed to different network interfaces based on well-known routing algorithms, and that these routing algorithms could be simply and favorably utilized in conjunction with network security algorithms like those taught by Shwed (column 8 lines 39-49 and Fig 8).

As per claims 8-11, 12-15, and 16, Shwed (US 5606668) describes a security system for a computer network that implements packet filtering (column 3, lines 59-65). Shwed teaches that his system applies a particular security rule to an incoming packet (column 7, lines 14-24) based on data extracted from the incoming packet (column 8 lines 39-49 and Fig 8).

As per claims 8, 9, 10, 13, and 14, Shwed does not explicitly teach the use of multiple independent security policies, administered by separate administrators and applied to different groups. However, Shwed further teaches (column 4, lines 27-67) that a system administrator may create security rules, and may designate that network objects be separated into sub-groups or domains, where sub-groups may utilize different sets of security rules (column 4, lines 23-26 and lines 50-57) which would implement multiple sets

of security policies. (Shwed uses as an example a communication group composed of a company's CEO, CFO, directors; security rules could be set up in the Shwed system to allow direct communication by this group, but not others, to a finance group (column 4, lines 59-63).) It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to allow the creation of specific security rules for a particular sub-group of network objects, because this could be accomplished with little modification to the Shwed system, and because the creation of independent security policies by the creation of multiple sets of rules would give users of the Shwed system the benefits of hierarchies of security.

As per claims 11, 15, and 16, although Shwed does not explicitly teach that only the administrator of a domain is allowed to modify the security policy rules for that domain, it would have been obvious to one of ordinary skill in the art, at the time the invention was made, to restrict the creation of security rules for a particular sub-group of network objects to a particular system administrator, because this could be accomplished with little, if any, modification to the Shwed system, and because the creation of rules by a specialist in a particular domain would give the benefits of increased security and confidence in the Shwed system.

### *Response to Arguments*

3. Applicant's arguments filed 12 Nov. 1999 have been fully considered but they are not persuasive.

Applicant argues that the claimed invention "provides a hierarchical rule selection procedure" (p. 2, line 6) which is distinct from the teachings of Shwed and which would not have been obvious to one ordinary skill in the art at the time the invention was made. However, applicant fails to disclose in his specification a rule selection procedure distinct from Shwed or not readily known in the art. Applicant's specification states "In rule processing for a packet, the rules are applied sequentially until a rule is found which is satisfied by the packet..." (p.6, lines 10-11). This method would have been well known in the art at the time the invention was made. Further, rule selection in packet filtering firewall systems at the time the invention was made was routinely based on data fields contained in the packet. The applicant's disclosure does not teach a different rule selection method.

As discussed above, Shwed teaches that his system may be used to create multiple security areas (domains) within a group of networks. It would have been obvious to one of ordinary skill in the art at the time the invention was made that different rules having different packet selection criteria would have to applied to different security domains. It would have been obvious to one of ordinary skill in the art at the time the invention was made that the selection of particular rule-based criteria would necessarily be based on data (address fields, control fields, etc.) contained in the packet or on data closely associated with the packet, such as the packet's hardware interface address.

As discussed above, Shwed clearly contemplates that certain groups of persons may have higher access privileges than others, and the Shwed system teaches how to implement such

hierarchical levels of access.

*Conclusion*

**4. THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

**Any response to this action should be mailed to:**

Commissioner of Patents and Trademarks  
Washington, D.C. 20231

**or faxed to:**

(703) 308-9051, (for formal communications intended for entry)

**Or:**

(703) 305-9731, (for informal or draft communications, please label "PROPOSED" or "DRAFT")



Hand delivered responses should be brought to Crystal Park II, 2121 Crystal Drive VA  
sixth Floor (Receptionist)

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

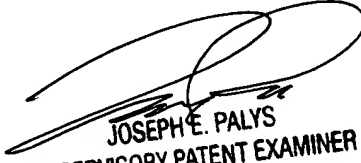
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Robert Crockett whose telephone number is (703) 305-6107. The examiner can normally be reached Monday-Thursday from 7:30 AM to 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Palys, can be reached at (703) 305-9685. The fax number for this Group is (703) 305-3718.

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703) 305-9618.

Robert G. Crockett

23 December 1999



JOSEPH E. PALYS  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2700